Google Scholar BETA

Web Images Video News Maps more »

galois field aes s-box Search

Advanced Scholar Search
Scholar Preferences
Scholar Help

Scholar **All articles** - Recent articles Results **1** - **10** of about **708** for **galois field aes s-box**. (**0.15** se

All Results
A Elbirt
A Satoh
S Morioka
V Rijmen
W Yip

An ASIC implementation of the **AES** SBoxes - all 3 versions »
J Wolkerstorfer, E Oswald, M Lamberger - Proc. RSA Conference, 2002 - Springer
... provides the mathematical background of the finite **field** arithmetic and the computation of the **AES** SBoxes in Sect. 2. The building blocks of an **SBox** and the ...
Cited by 69 - Related Articles - Web Search - BL Direct

A 10-Gbps full-**AES** crypto design with a twisted BDD **S-Box** architecture - all 9 versions »
S Morioka, A Satoh - Very Large Scale Integration (VLSI) Systems, IEEE ..., 2004 - ieeexplore.ieee.org
... constructing compact inversion circuits over **Galois field** have been ... the composite **field** (or tower **field**) inversion [10 ... for achieving 10-Gbps **AES** circuits due to ...
Cited by 35 - Related Articles - Web Search - BL Direct

Essential algebraic structure within the **AES** - all 19 versions »
S Murphy, MJB Robshaw - Advances in Cryptology-CRYPTO, 2002 - Springer
... BES, Al- gebraic Structure, (Finite) **Galois Field**, (**Field**) Conjugate, Multivariate ... in F for non-zero **field** elements with 0 ... c) The output of the **AES S-Box** is (L ...
Cited by 88 - Related Articles - Web Search - BL Direct

An Optimized **S-Box** Circuit Architecture for Low Power **AES** Design - all 4 versions »
S Morioka, A Satoh - Proc. CHES, 2002 - Springer
... reductions using mathematical theorems over **Galois fields** (GF) [12 ... be used to create compact **AES** implementations [9 ... detail of the composite **field** technique will ...
Cited by 32 - Related Articles - Web Search - BL Direct

A Compact Rijndael Hardware Architecture with **S-Box** Optimization - all 4 versions »
A Satoh, S Morioka, K Takano, S Munetoh - Proc. ASIACRYPT, 2001 - Springer
... The **AES** has to be embeddable not only in high-end servers but also in low-end consumer ...
An **S-Box** is the multiplicative inverse of a **Galois field** GF(2 ...
Cited by 99 - Related Articles - Web Search - BL Direct

A Side-Channel Analysis Resistant Description of the **AES S-box** - all 4 versions »
E Oswald, S Mangard, N Pramstaller, V Rijmen - Fast Software Encryption, 12th International Workshop, FSE, 2005 - Springer
... Our approach is based on shifting the computation of the finite **field** inversion in the **AES S-box** down to GF(4). In this **field**, the inversion is a linear ...
Cited by 13 - Related Articles - Web Search

Integrated design of **AES** (Advanced Encryption Standard) encrypter and decrypter - all 5 versions »
CC Lu, SY Tseng - Application-Specific Systems, Architectures and Processors, ..., 2002 - ieeexplore.ieee.org

... the matrix M. By the finite **field** inverse matrix ... SubBytes/InvSubBytes module (inverse-optional **S-box** module), capable ... use in encryption and decryption of **AES**. ...
Cited by 37 - Related Articles - Web Search

4.2 Gbit/s single-chip FPGA implementation of **AES** algorithm - all 3 versions »
F Rodriguez-Henriquez, NA Saqib, A Diaz-Perez - Electronics Letters, 2003 - ieeexplore.ieee.org
... The **AES S-box** is a 256-entry table composed of ... while IAF +MI computes the Inverse **S-box** needed for ... where xtime(v) represents the finite **field** multiplication of ...
Cited by 19 - Related Articles - Web Search - BL Direct

Minimum area cost for a 30 to 70 Gbits/s **AES** processor - all 9 versions »
A Hodjat, I Verbauwhede - VLSI, 2004. Proceedings. IEEE Computer society Annual ..., 2004 - ieeexplore.ieee.org
... using the pipelined implementation of the composite **Galois Field** ... design of the composite
field implementation of ... to 100 Gbits/s Throughput **AES** Processor', 37 ...
Cited by 23 - Related Articles - Web Search

Provably Secure Masking of **AES** - all 11 versions »
J Blomer, JG Merchan, V Krummel - Selected Areas in Cryptography, 11th International Workshop, ..., 2004 - Springer
... using arithmetic operations defined over some finite **field** into a ... k that is co-prime to p. The **field** F ... Combinational Logic Design for **AES S-Box** on Masked Data. ...
Cited by 27 - Related Articles - Web Search

Goooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

galois field aes s-box Search

Google Home - About Google - About Google Scholar